IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | ) | |
| | ) | |
| **v.** | ) | **Criminal No.: 2:24-cr-** 26 |
| | ) | |
| | ) | **Racketeer Influenced and Corrupt** |
| **ERIC HOURRUITINEL,** | ) | **Organizations (RICO) Conspiracy** |
| | ) | **18 U.S.C. § 1962(d)** |
| | ) | |
| | ) | |
| **Defendant.** | ) | **Criminal Forfeiture** |
| | ) | **18 U.S.C. § 1963(a) and (m)** |

## CRIMINAL INFORMATION

THE UNITED STATES ATTORNEY CHARGES THAT:

### COUNT ONE
(Racketeer Influenced and Corrupt Organizations (RICO) Conspiracy)

### The Enterprise

1. Beginning in or about 2014, and at all times relevant to this Criminal Information, **ERIC HOURRUITINEL** (**"HOURRUITINEL"**), the defendant, and others known and unknown to the United States, were members and associates of a criminal organization, (hereinafter, "The Enterprise"), which was engaged in, among other things, acts of money laundering, access device fraud, bank fraud, interstate transportation in aid of racketeering, interstate transportation of stolen goods or moneys, and sale or receipt of stolen goods or moneys, and which operated in the states of Virginia, Florida, Maryland, North Carolina, South Carolina, California, Washington, Nevada, Illinois, Arizona, Oklahoma, Texas, Arkansas, Missouri, and elsewhere.

2. This criminal organization, including its leadership, membership, and associates, constituted an "enterprise," as defined by 18 U.S.C. § 1961(4), that is, a group of individuals associated in fact. The Enterprise constituted an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives of the Enterprise. This Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

Background

3. The Enterprise engaged in gas pump skimming operations throughout the United States to fraudulently acquire credit and debit card information. Gas pump skimming involves the covert installation of portable credit and debit card-reading devices, called "skimming devices," in or on gas pumps and, in this case, pumps located within the Eastern District of Virginia and elsewhere.

4. A skimming device intercepts, reads, and records the information ("track data") encoded on a credit or debit card's magnetic strip while the skimming device is connected to a gas pump card-reading apparatus. Track data includes, but is not limited to, financial information such as credit and debit card account information and personal identification, including the customer's Personal Identification Number ("PIN") access codes and zip codes entered by legitimate customers during transactions at gas station locations.

5. Track data can be purchased, sold, and transferred electronically and can be used to create cloned credit and debit cards. Cloned credit and debit cards are counterfeit credit and debit cards created using a combination of electronic hardware and software to encode stolen track data onto cards with magnetic strips.

6. Skimming revenue includes, but is not limited to, gift cards, merchandise, and cash obtained using cloned credit and debit cards.

7. Cloned credit and debit cards may be used during cash-out operations to obtain skimming revenue from compromised bank accounts. Cash-out operations include using cloned credit and debit cards at automatic teller machines ("ATMs"), banks, point-of-sale kiosks, and fences to illegally obtain skimming revenue from the compromised bank accounts of legitimate owners of the credit and debit cards.

8. Skimming operations include, but are not limited to, scouting locations for the installation of skimming devices, monitoring skimming devices, retrieving track data from skimming devices, uninstalling skimming devices, creating cloned credit and debit cards using track data obtained from skimming devices, cash-out operations, and using fences to exchange illicit goods for cash.

9. A fence is a middleman who buys stolen goods, including but not limited to gift cards, track data, and electronics, for less than market value to later resell for a profit.

The Enterprise Structure

10. The Enterprise was founded by co-conspirator 1 ("CC1") in the Miami, Florida area in or about 2014 and was led by CC1 and other higher-level members.

11. Membership in the Enterprise was contingent upon approval by CC1. Existing members "vouched" for new or prospective members, who had to demonstrate their value and loyalty to the Enterprise by assisting Enterprise members and associates with skimming operations and related tasks, such as providing transportation for Enterprise members and their associates.

12. CC1's leadership over the Enterprise stemmed from his extensive experience with skimming operations and other fraud schemes, including credit card fraud, skimming device fraud, buying stolen information, and converting stolen information to gift cards, merchandise, or cash and his ability to maintain a clandestine presence.

13. The Enterprise operated with a tiered structure wherein members and associates of the Enterprise were required to share a portion of the revenue they obtained through their participation in skimming operations with Enterprise leadership, including CC1. Enterprise members achieved higher status by demonstrating their loyalty, reliability, and trustworthiness, and by a history of completing successful cash-out operations. Higher-level Enterprise members were given more responsibility, granted access to more information about skimming operations, and given more profitable track data.

14. To maintain his status within and control of the Enterprise, CC1 limited the flow of information to certain members and associates of the Enterprise on a need-to-know basis. CC1 used different, temporary phone numbers to communicate directly with members and associates of the Enterprise and did not disclose his last name. CC1 also only communicated with some Enterprise members and associates indirectly through other Enterprise members and associates. Therefore, some lower-level members and associates of the Enterprise knew that certain individuals led the Enterprise but did not necessarily know CC1 by name.

15. CC1 and other Enterprise members maintained a business relationship with co-conspirator 2 ("CC2"), an associate of the Enterprise, who assembled and sold skimming devices for profit. Enterprise members and associates, including CC1, routinely purchased skimming devices from CC2.

16. CC2 also operated as a fence for Enterprise members and associates by purchasing items obtained from skimming operations for less-than-market value.

Manner and Means of the Enterprise

17. The manner and means by which members and associates of the Enterprise conducted and participated in the conduct of the affairs of the Enterprise included, but were not limited to, the following:

a. Enterprise members and associates used skimming devices on gas pumps.

b. Higher-level Enterprise members determined the locations at which to install the skimming devices by using cellular telephones and computers to search the internet for photographs of potential target locations compatible with the skimming devices.

c. Enterprise members and associates traveled, typically via airplane, to locations throughout the United States to install skimming devices.

d. Early skimming devices, used from in or about 2014 until in or about 2018, did not have wireless capability and needed to be physically removed from the gas pump to download the track data. Therefore, Enterprise members and associates had to physically uninstall the skimming devices from gas pumps to capture the track data of cards used there. Later gas pump skimming devices, available in or around 2018, still required that the skimming device be physically installed, but the updated devices had wireless capability. Therefore, the skimming device could transmit track data remotely via cellphone or computer; that is, without the device being removed from the gas pump. The updated skimming devices could also capture zip codes and/or PINs associated with credit and debit cards. Therefore, when using cloned credit and debit cards, Enterprise members and associates no longer had to provide identifications to make purchases, could also obtain cash from ATMs, and could get cash back as part of transactions.

e. Enterprise members and associates created cloned credit and debit cards using the stolen track data.

f. Enterprise members and associates purchased large quantities of gift cards and expensive goods using the cloned credit and debit cards.

g. To evade detection by law enforcement and financial institutions, Enterprise members and associates delayed use of the stolen track data for a short period of time.

h. To minimize the number of transactions made with the stolen track data and to evade detection, Enterprise members and associates purchased large quantities of gift cards and expensive items, including Apple iPads and laptops.

i. Enterprise members and associates then sold these items below market price to fences who paid cash.

j. To maximize the potential gain, Enterprise members and associates sorted the card numbers from the stolen track data into categories, by searching the leading digits of the card numbers using the internet and/or other sources to determine card types. Numbers associated with higher value credit cards, including "Gold," "Platinum," or "Business" cards, were distributed to higher-level Enterprise members and associates.

k. Members and associates of the Enterprise used e-mail to share and/or distribute stolen track data to other members and associates of the Enterprise and others known and unknown to the United States.

Purposes of the Enterprise

18. The purposes of the Enterprise included, but were not limited to, the following:

a. enrichment of members and associates of the Enterprise through skimming operations involving the illicit procurement of gift cards and other goods generated by the skimming operations;

b. moving, disguising, and protecting financial proceeds of the Enterprise's skimming operations by converting proceeds of the illicit operations into untraceable cash; and

c. concealing the Enterprise's scheme to defraud financial institutions by converting stolen track data into gift cards, money orders, and/or cash.

The Racketeering Conspiracy

19. Beginning in or about 2014 and continuing through on or about the date of the filing of this Criminal Information, both dates being approximate and inclusive, within the Eastern District of Virginia, and elsewhere, **ERIC HOURRUITINEL ("HOURRUITINEL")**, the defendant, with other persons known and unknown to the United States, each being a person employed by and associated with the Enterprise, which was engaged in, and the activities of which affected, interstate and foreign commerce, knowingly and intentionally conspired with each other, and others known and unknown to the United States, to violate 18 U.S.C. § 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the Enterprise through a pattern of racketeering activity, as defined in 18 U.S.C. §§ 1961(1) and (5), which pattern of racketeering consisted of multiple acts indictable under:

a. 18 U.S.C. § 1029 (relating to fraud and related activity in connection with access devices);

b. 18 U.S.C. § 1343 (relating to wire fraud);

c. 18 U.S.C. § 1344 (relating to financial institution fraud);

d. 18 U.S.C. § 1952 (relating to racketeering);

e. 18 U.S.C. § 1956 (relating to laundering of monetary instruments);

f. 18 U.S.C. § 2314 (relating to interstate transportation of stolen property); and

g. 18 U.S.C. § 2315 (relating to interstate transportation of stolen property).

20. It was part of the conspiracy that the defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the Enterprise.

Overt Acts

21. In furtherance of the racketeering conspiracy, and to affect the object and purposes thereof, **ERIC HOURRUITINEL ("HOURRUITINEL")**, the defendant, and others known and unknown to the United States, committed and caused to be committed various overt acts within the Eastern District of Virginia and elsewhere, including, but not limited to, the following:

1) In or about 2014, CC1 and co-conspirator 3 ("CC3") met an individual known to the United States at a gas station in the Miami, Florida area where CC1 purchased a Mini-123 skimming device for approximately $8,000.

2) In or about 2014, CC1 directed CC3 to travel to Maryland to test the Mini-123 skimming device.

3) In or about 2014, CC3 traveled to Maryland, where he connected the Mini-123 skimming device to a gas pump and collected track data for approximately one week.

4) From about 2014 through about 2017, Enterprise members and associates used the Mini-123 skimming device to conduct skimming operations at gas stations around the United States.

5) In or about 2017, CC2 assembled an HC-05 skimming device using materials purchased from an internet electronics retailer, which he sold to members of the Enterprise.

6) In or about September 2017, CC3 and other Enterprise members and associates purchased a skimming device from CC2 and installed it in an Exxon gas station pump in the Hardeeville, South Carolina area.

7) In or about 2017, CC3 and CC1 installed skimming devices obtained from CC2 at multiple gas pumps along the I-95 corridor in Virginia, including in and around Ruther Glen, Virginia.

8) In or about April 2018, CC3, co-conspirator 4 ("CC4"), and other Enterprise members and associates traveled to Virginia to conduct a skimming operation.

9) On or about April 21, 2018, CC3, CC4, and other Enterprise members and associates drove in and around Virginia to scout locations to use cloned bank cards, including Norfolk, Virginia.

10) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used Advantage Financial Federal Credit Union information belonging to victim R.M. to make an unauthorized cash withdrawal at a grocery store in Norfolk, Virginia.

11) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used SunTrust Bank information belonging to victim J.B. to make an unauthorized purchase of a prepaid credit card at a grocery store in Chesapeake, Virginia.

12) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used SunTrust Bank information belonging to victim J.B. to make an unauthorized cash withdrawal at a grocery store in Chesapeake, Virginia.

13) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used Police and Fire Federal Credit Union information belonging to victim M.P. to make an unauthorized cash withdrawal at a grocery store in Virginia Beach, Virginia.

14) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used Pentagon Federal Credit Union information belonging to victim K.M. to make an unauthorized purchase of a prepaid credit card at a grocery store in Virginia Beach, Virginia.

15) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used Bank of America information belonging to victim D.L.W. to attempt to make an unauthorized cash withdrawal at a grocery store in Virginia Beach, Virginia.

16) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used Union Bank information belonging to victim A.S. to make an unauthorized cash withdrawal at a restaurant in Exmore, Virginia.

17) On or about April 21, 2018, CC3, CC4, and other members and associates of the Enterprise used Zenith/Union Bank information belonging to victim S.M. to make an unauthorized cash withdrawal at a restaurant in Exmore, Virginia.

18) On or about April 22, 2018, CC3, CC4, and other members and associates of the Enterprise used BB&T Bank information belonging to victim T.C. to attempt to make an unauthorized cash withdrawal at a restaurant in Exmore, Virginia.

19) On or about May 14, 2018, a member of the Enterprise rented a vehicle in and around Fort Lauderdale, Florida and listed CC3 as an authorized alternate driver.

20) On or about May 14, 2018, CC3 and other members and associates of the Enterprise possessed cloned credit and debit cards, cash, merchandise, and a laptop containing stolen track data, in or around Charlotte, North Carolina.

21) On or about May 29, 2018, CC2 purchased materials used to manufacture skimming devices from an internet electronics retailer.

22) In or about October 2018, CC3, CC4, co-conspirator 5 ("CC5"), and another Enterprise member transported approximately $150,000 of proceeds from a skimming operation from California to Arizona via automobile.

23) In or about October 2018, CC1 transported approximately $250,000 obtained from a skimming operation from California to Nevada via automobile.

24) In or about October 2018, CC1 and others known and unknown to the United States deposited approximately $250,000 obtained from a skimming operation into bank accounts in the Las Vegas, Nevada area.

25) On or about November 7, 2018, Enterprise members and associates shared stolen track data using e-mail.

26) On or about November 20, 2018, an Enterprise member sent an e-mail containing track data from approximately 300 stolen credit and debit cards to an e-mail account associated with CC2.

27) On or about November 29, 2018, an Enterprise member sent an e-mail containing track data from approximately 80 stolen credit and debit cards to an e-mail account associated with CC2.

28) On or about November 30, 2018, an Enterprise member sent an e-mail containing track data from approximately 600 stolen credit and debit cards to an e-mail account associated with CC2.

29) On or about December 4, 2018, CC4 traveled via plane from Florida to California to conduct a skimming operation.

30) On or about December 5, 2018, **HOURRUITINEL**, co-conspirator 6 ("CC6"), and CC5 traveled via plane from Florida to California to conduct a skimming operation.

31) On or about December 5, 2018, CC1 traveled via plane from Florida to Nevada.

32) On or about December 5, 2018, CC1 rented a vehicle in Reno, Nevada for the period December 5, 2018, through December 12, 2018.

33) On or about December 5, 2018, CC1 booked hotel accommodations in Lathrop, California for the period December 5, 2018, through December 8, 2018.

34) On or about December 5, 2018, CC3 booked hotel accommodations in California for the period of December 5, 2018, through December 10, 2018.

35) On or about December 5, 2018, CC3 rented a vehicle in California for the period December 5, 2018, through December 9, 2018.

36) On or about December 5, 2018, CC4 rented a vehicle in California for the period December 5, 2018, through December 13, 2018.

37) Between on or about December 5, 2018, and on or about December 13, 2018, CC1, CC4, CC5, CC6, **HOURRUITINEL**, and CC3 drove the rental vehicles in and around California scouting locations and installing skimmers on gas pumps.

38) Between on or about December 6, 2018, and on or about December 13, 2018, CC4 and **HOURRUITINEL** used cellular phones and other electronic devices to search for businesses where Enterprise members could conduct cash-out operations.

39) Between on or about December 6, 2018, and on or about December 13, 2018, CC1, CC4, CC5, CC6, **HOURRUITINEL**, and CC3 purchased gift cards with stolen track data.

40) On or about December 6, 2018, CC5 rented a vehicle in California for the period December 6, 2018, through December 13, 2018.

41) On or about December 6, 2018, CC5 booked hotel accommodations in the Lathrop, California area for the period of December 6, 2018, through December 9, 2018.

42) Between on or about December 6, 2018, and on or about December 13, 2018, CC1, CC3, **HOURRUITINEL**, CC4, CC5, CC6, and other Enterprise members and associates installed skimming devices on gas pumps in the San Francisco, California area.

43) Between on or about December 6, 2018, and on or about December 13, 2018, CC1, CC3, **HOURRUITINEL**, CC4, CC5, CC6, and other Enterprise members and associates obtained track data from the skimming devices installed at gas pumps in the San Francisco, California, arca.

44) Between on or about December 6, 2018, and on or about December 13, 2018, CC1, CC3, **HOURRUITINEL**, CC4, CC5, CC6, and other Enterprise members and associates created cloned credit and debit cards from the stolen track data obtained from skimming devices installed at gas pumps in the San Francisco, California.

45) On or about December 6, 2018, CC4 conducted a Google Maps search for a Home Depot location in Livermore, California where Enterprise members and associates could cash out cloned credit and debit cards.

46) On or about December 6, 2018, **HOURRUITINEL** conducted a Google Maps search for a Home Depot location in Sacramento, California where Enterprise members and associates could cash out cloned credit and debit cards.

47) On or about December 7, 2018, CC4 conducted a Google Maps search for a Home Depot location in Elk Grove, California where Enterprise members and associates could cash out cloned credit and debit cards.

48) On or about December 7, 2018, **HOURRUITINEL** conducted a Google Maps search for a Home Depot location in Lodi, California where Enterprise members and associates could cash out cloned credit and debit cards.

49) On or about December 8, 2018, CC4 used Google Maps to search for a Home Depot location in Livermore, California, where Enterprise members and associates could cash out cloned credit and debit cards.

50) On or about December 11, 2018, **HOURRUITINEL** booked hotel accommodations in Stockton, California for the period of December 11, 2018, through December 14, 2018.

51) On or about December 13, 2018, CC1, CC4, CC5, CC6, and **HOURRUITINEL** traveled via plane from California to Florida, carrying gift cards they had obtained fraudulently on their persons and in their luggage.

52) On February 8, 2019, an e-mail account associated with CC3 sent an e-mail containing track data from approximately 2,500 stolen credit and debit cards to an e-mail account associated with co-conspirator 7 ("CC7").

53) On February 12, 2019, an e-mail account associated with CC7 sent an e-mail containing track data from approximately 50 stolen credit or debit cards.

54) On February 19, 2019, **HOURRUITINEL** traveled via plane from the Miami, Florida area to the San Francisco, California area to conduct a skimming operation.

55) On or about February 19, 2019, **HOURRUITINEL** and CC3 rented vehicles in the San Francisco, California area for the period February 19, 2019, through February 26, 2019.

56) On or about February 19, 2019, CC1 rented a vehicle in the Seattle, Washington area for the period February 21, 2019, through February 23, 2019.

57) On February 20, 2019, CC5 and CC6 traveled together via plane from the Miami, Florida area, to the Seattle, Washington, area to conduct a skimming operation.

58) On or about February 20, 2019, CC4 traveled from the Miami, Florida area to the Seattle, Washington area to conduct a skimming operation.

59) On February 21, 2019, CC1 traveled from the Miami, Florida area to the San Francisco, California area to conduct a skimming operation.

60) On or about February 21, 2019, CC1, **HOURRUITINEL**, and CC3 traveled from the San Francisco, California area, to the Seattle, Washington, area to conduct a skimming operation.

61) On or about February 21, 2019, CC5 rented a vehicle in the Seattle, Washington area for the period February 21, 2019, through February 25, 2019, and returned the vehicle to the San Francisco, California area.

62) Between on or about February 21, 2019, through on or about February 24, 2019, CC1, CC3, **HOURRUITINEL,** co-conspirator 8 ("CC8"), CC5, CC6, and other Enterprise members searched for gas stations where they could install skimming devices in the Seattle, Washington area.

63) On or about February 22, 2019, CC1 conducted internet searches to scout for a Chevron gas station in the Tacoma, Washington area, and a Mobil gas station in the Auburn, Washington area.

64) Between on or about February 22, 2019, and on or about February 23, 2019, on approximately 20 separate occasions, **HOURRUITINEL** used Google Maps to search for Lowe's Home Improvement stores in cities located in Washington state where Enterprise members and associates could cash out cloned credit and debit cards.

65) On or about February 22, 2019, CC8 rented a vehicle in the Seattle, Washington area for the period February 22, 2019, through February 23, 2019.

66) On February 23, 2019, CC1 traveled via plane from the Seattle, Washington area, to the Miami, Florida area.

67) Between on or about February 24, 2019, and on or about February 25, 2019, CC4, CC5, CC6, **HOURRUITINEL**, and CC3 traveled from the Seattle, Washington area to the San Francisco, California with proceeds from the skimming operation.

68) On February 24, 2019, CC1 traveled via plane from the Miami, Florida area to the San Francisco, California area to conduct a skimming operation.

69) On or about February 24, 2019, CC5 rented a hotel room from February 24, 2019, to February 25, 2019, in the Grants Pass, Oregon area as part of a skimming operation.

70) On or about February 25, 2019, CC1 rented a hotel room and a vehicle for the period of February 25, 2019, through February 26, 2019, in the San Francisco, California area.

71) Between on or about February 25, 2019, and February 26, 2019, CC4 and **HOURRUITINEL** conducted internet searches to scout for various stores and gas stations in and around the San Francisco, California area.

72) On or about February 25, 2019, CC2 purchased materials used to manufacture skimming devices from an internet electronics retailer.

73) On February 26, 2019, CC6, **HOURRUITINEL**, CC1, CC4, and another Enterprise member traveled via plane from the San Francisco, California area to the Los Angeles, California area to conduct a skimming operation. CC4 and another member of the Enterprise flew on tickets purchased from the same reservation.

74) On or about February 27, 2019, CC1 rented a room at the New York-New York Hotel in Las Vegas, Nevada from February 27 to March 4, 2019. CC3 was listed on the reservation as sharing the room.

75) Between on or about March 1, 2019, and March 3, 2019, on approximately 20 separate occasions, **HOURRUITINEL** used Google Maps to search for Lowe's Home

Improvement stores located in various Arizona towns and cities where Enterprise members and associates could cash out cloned credit and debit cards obtained from part of a skimming operations.

76) On March 7, 2019, CC5 and CC6 traveled via plane from the Phoenix, Arizona area, to the Chicago, Illinois area to conduct a skimming operation. CC5 and CC6 flew on tickets purchased from the same reservation.

77) Between on or about March 7, 2019, and on or about March 12, 2019, CC1, CC5, CC6, **HOURRUITINEL**, and other members of the Enterprise installed skimming devices on gas pumps in the Chicago, Illinois area.

78) Between on or about March 7, 2019, and on or about March 12, 2019, CC1, CC5, CC6, **HOURRUITINEL**, and other members of the Enterprise obtained track data from the skimming devices installed at gas pumps in the Chicago, Illinois area.

79) Between on or about March 7, 2019, and on or about March 12, 2019, CC1, CC5, CC6, **HOURRUITINEL**, and other Enterprise members and associates used track data obtained from skimming devices installed at gas pumps in the Chicago, Illinois area to create cloned credit and debit cards.

80) On March 8, 2019, CC1 traveled via plane from the San Francisco, California area to the Chicago, Illinois area to conduct a skimming operation.

81) On or about March 8, 2019, CC1 and CC5 each rented vehicles for the period March 8, 2019, through March 11, 2019, in the Chicago, Illinois area.

82) On March 8, 2019, CC8 traveled via plane from the Phoenix, Arizona area to the Chicago, Illinois area to conduct a skimming operation.

83) On March 9, 2019, **HOURRUITINEL** traveled via plane from the Fort Myers, Florida area to the Chicago, Illinois area to conduct a skimming operation.

84) On or about March 9, 2019, **HOURRUITINEL** rented a vehicle for the period of March 9 through March 12, 2019, in the Chicago, Illinois area.

85) Between on or about March 10, 2019, and March 11, 2019, **HOURRUITINEL** used Google Maps to search for Lowe's Home Improvement and Home Depot stores in cities located in Illinois where Enterprise members and associates could cash out cloned credit and debit cards.

86) On March 11, 2019, CC1 and CC6 traveled via plane from the Chicago, Illinois area to the Miami, Florida area.

87) On March 12, 2019, **HOURRUITINEL** traveled via plane from the Chicago, Illinois area to the San Francisco, California area to conduct skimming operations.

88) On or about April 3, 2019, CC1 and CC7 flew from Miami to the San Francisco area to conduct a skimming operation.

89) On or about April 15, 22, 24, and 25, 2019, CC3 used e-mail to share stolen track data with CC2.

90) On or about April 16, 2019, **HOURRUITINEL** traveled to the St. Louis area to conduct a skimming operation.

91) On or about April 18, 2019, CC1 flew from Miami to the St. Louis, Missouri area to conduct a skimming operation.

92) On or about April 19, 2019, **HOURRUITINEL** received stolen track data from CC3 using e-mail.

93) Between on or about May 2, 2019, and May 5, 2019, **HOURRUITINEL** used Google Maps to search for Lowe's Home Improvement in cities located in Tennessee where he could cash out cloned credit and debit cards.

94) On or about May 8, 2019, CC4 possessed approximately five cloned credit and debit cards with handwritten PINs on the back side of the cards.

95) On or about May 8, 2019, CC4 possessed approximately eight credit card and PIN combinations and photographs of credit cards in his cellular phone.

96) On or about May 10, 2019, CC7 traveled from Miami to the St. Louis, Missouri area to conduct a skimming operation.

97) Between on or about May 24, 2019, and May 29, 2019, **HOURRUITINEL** used Google Maps to search for Lowe's Home Improvement stores in cities located in Oklahoma, Texas, and Arkansas, where he could cash out cloned credit and debit cards.

98) On or about May 25, 2019, **HOURRUITINEL** and CC1 installed skimming devices in and around St. Louis, Missouri.

99) Between on or about May 30, 2019, and June 1, 2019, **HOURRUITINEL** used Google Maps to search for Lowe's Home Improvement stores in cities located in Missouri where he could cash out cloned credit and debit cards.

100) On or about June 30, 2019, **HOURRUITINEL** used e-mail to share stolen track data with CC1.

All in violation of Title 18, United States Code, Section 1962(d).

**CRIMINAL FORFEITURE**

1. Upon conviction on Count One, the defendant, **ERIC HOURRUITINEL ("HOURRUITINEL")**, shall forfeit to the United States, pursuant to 18 U.S.C. § 1963(a)(1)-(3):

a. any and all interest defendant has acquired or maintained in violation of 18 U.S.C. § 1962;

b. any and all interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over, any enterprise which defendant established, operated, controlled, conducted, or participated in the conduct of, in violation of 18 U.S.C. § 1962; and

c. any and all property constituting, or derived from, any proceeds obtained, directly or indirectly, from racketeering activity in violation of 18 U.S.C. § 1962.

2. This property includes, but is not limited to, a forfeiture money judgment against the convicted defendant(s) in an amount determined by the Court to represent the total amount of proceeds obtained as a result of the violation.

4. This property includes, but is not limited to, a forfeiture money judgment against the convicted defendant(s) in an amount determined by the Court to represent the total amount of property involved in the offense, or any property traceable to such property.

4. Pursuant to 18 U.S.C. § 1963(m) and 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b), if any of the property subject to forfeiture described in paragraphs 2 and 3, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States intends to seek forfeiture of any other property of the defendant up to the value of the forfeitable property.

In accordance with 18 U.S.C. §§ 982(a)(1), 1963(a), 1963(m); 21 U.S.C. § 853(p); Fed. R. Crim. P. 32.2.

Respectfully submitted,

JESSICA D. ABER
UNITED STATES ATTORNEY

By: _____

KRISTEN S. TAYLOR
Pennsylvania State Bar No. 326039
Assistant United States Attorney
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510-1671
Telephone: 757-441-6331
Fax: 757-441-6689
E-mail: Kristen.Taylor2@usdoj.gov

Date: April 5, 2024

_____

BEN TONKIN
New York State Bar No. 5203880
Trial Attorney
Violent Crime and Racketeering Section
U.S. Department of Justice
1301 New York Ave., N.W.
Washington, DC 20530
Telephone: 202-514-3594
E-mail: Ben.Tonkin@usdoj.gov

_____

CLAYTON D. LAFORGE
Pennsylvania State Bar No. 84075

Assistant United States Attorney
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510-1671
Telephone: 757-441-6331
Fax: 757-441-6689
E-mail: Clayton.LaForge@usdoj.gov